October 3, 2013

Minnesota Bureau of Criminal Apprehension Policy on Appropriate Use of Systems and Data

Contents

In support of criminal justice agencies and other authorized users, the Minnesota Bureau of Criminal Apprehension (BCA) operates a number of data repositories and a secure network. This system allows authorized users to access data from state and federal sources in order to perform their official functions. In some instances, the statute that created the repository authorizes the access to and use of the data. In other instances, access to the data is governed by the provisions found in the Minnesota Government Data Practices Act, Minnesota Statutes, Chapter 13 and Minnesota Statutes, section 299C.46.

A. Purpose

The purpose of this policy is to set the standards and guidelines for appropriate use of the repositories and secure network, document the processes to be followed to determine if the use is appropriate and to provide penalties for failure to meet the standards. The BCA's goal is that authorized agencies and users be in full compliance with all requirements. Agencies and users that fail to comply with this policy will be subject to the sanctions described later.

This Policy and the appendix will be periodically revised as issues and examples are identified. Notice that revised documents are available will be sent to agency heads.

B. Definitions

As used in this policy, the following terms have the meaning given.

"Appropriate use" means the agency that employs the individual user is eligible under the applicable statutes and regulations to have access to the secure network and the data, and that the data have been retrieved as part of an employee's work assignment or are retrieved to share the data with another entity authorized by law to receive them. If an agency has a more restrictive policy on access and/or sharing, the employee must also follow the agency policy.

"Authorized agency" means a criminal justice agency or noncriminal justice agency as defined in Minnesota Statutes, section 299C.46.

"Follow up audit" means an audit of an agency following identification of issues identified during a routine audit or when inappropriate use has been found. A follow up audit can occur anytime within the three year audit cycle.

"Inappropriate use" means any use that is not an "appropriate use" or for which there is no acceptable lawful explanation of or documentation of why the transaction was conducted. Examples or a lawful explanation include "assigned to traffic enforcement," "assigned to Safe and Sober campaign," or "to determine eligibility for benefits."

"Intentional" means that an employee knowingly behaves in a manner that is inappropriate or repeats a behavior after being informed that the behavior is not acceptable. Determining the intent of the employee is done either by the agency or the BCA.

"Non-compliant" means an agency has not taken the necessary steps to conduct the investigation or to resolve the issues identified during an audit or investigation.

"Unintentional" means that an employee unknowingly behaves in a way that results in inappropriate use.

C. Control of Access and Appropriate Use

Access to and use of data in BCA repositories or available from other repositories via the secure network is controlled by one or more of the following:

- A specific state statute – e.g. Minnesota Statutes, section 299C.40 controls the Comprehensive Incident-Based Reporting System (CIBRS)
- Minnesota Statutes, section 299C.46 controls the use of the secure network
- Federal regulations implemented through the FBI CJIS Security Policy
- *The Rules of Public Access to Records of the Judicial Branch* control access to court case information
- Policies adopted by other agencies concerning access to and use of that agency's data – e.g. Corrections' policies on access to the Statewide Supervision System (S^3).
- Terms of the contract between the agency and the BCA

A chart showing all of the repositories or tools with authorized users and examples of appropriate and inappropriate use is attached as Appendix 1.

It is never appropriate to retrieve data on yourself. Data practices procedures must be used to obtain data on you.

The BCA provides training on appropriate use of the various repositories and in some instances requires that users be certified to have access. Some of the systems that require certification also require re-certification. The BCA enforces all certification and re-certification requirements. The agency head is responsible

for ensuring that authorized employees review relevant training for use of the secure network and accessing the repositories as well as completing certification when required.

To ensure that all authorized agencies and users are in compliance with the applicable requirements, the BCA has a Training and Auditing Unit whose staff members are responsible for assisting agencies and their users as well as auditing transactions for compliance.

D. Audits

Currently, transactions involving Minnesota and federal criminal history and "Hot File" data are audited every three years as required by the FBI. Additional audits are done of agencies:

- ✓ with access to CIBRS;
- ✓ of Integrated Search Services users who access the S^3 ; and
- ✓ using a methodology that identifies patterns of use. For example, access to Driver and Vehicle Services (DVS) data via the secure network.

If issues are identified during an audit, the agency may be subject to follow up audits.

Evaluation of access and use can occur during an audit, as a result of a question asked by an agency's user, in response to an official agency request, following allegations of inappropriate use or based on transactions identified by the BCA's pattern analysis tool. Use will be reviewed at both an individual user and agency level.

Examples of issues that can result in a finding of inappropriate use or noncompliance include, but are not limited to:

- o Unintentional inappropriate use of data retrieved from BCA repositories or repositories reached via the BCA secure network
- o Unintentional inappropriate use of the secure network
- o Intentional inappropriate use of data retrieved from BCA repositories or repositories reached via the BCA secure network
- o Intentional inappropriate use of the secure network

- Retrieving data and providing it to an individual whose access to the system or network has been suspended
- Failure to ensure the security of the data and equipment used to retrieve the data
- Retrieval or sharing of data in a manner not authorized by the governing statute or federal regulation
- Failure to investigate allegations of inappropriate use presented by BCA to the agency
- Failure to request an extension to respond to an audit request
- Failure to respond to BCA requests for information about transactions performed by agency users
- Failure to address problems found during an audit or follow-up audit

If the failure to respond to BCA requests for information are due to litigation, the agency should inform the BCA of the litigation and provide an explanation once liability is determined or the case settles, whichever occurs first.

E. Sources of Possible Inappropriate Use

There are four ways that possible inappropriate use is identified for investigation and evaluation.

Audit of an agency

Inappropriate use discovered during an agency audit will be addressed as part of that audit and is subject to the requirements and sanctions in this Policy.

Allegations of inappropriate use to the BCA by an individual who is the subject of the data

When a member of the public alleges inappropriate use of data about that individual or the individual's minor child, the individual is directed to the BCA data practices process. If the individual completes the request form and meets the requirements for identification (notarization or in-person presentation with government-issued photo id), any data that are about the individual who has made the request, or their minor child, and which are contained in Archive Services are produced.

If the individual or their legal representative subsequently notifies the data practices analyst that they believe inappropriate use has occurred, the data practices analyst refers the individual to the MNJIS Executive Director.

The Executive Director will contact the agency head to give notice that inappropriate use allegations have been raised, that the individual has been advised to contact the agency head, request that the agency determine if inappropriate use has occurred and report any findings to the Executive Director. If the alleged inappropriate use involves data housed in a repository operated by another agency, the Executive Director will notify that other agency of the allegations. The Executive Director will also notify the Director of the Training and Auditing Unit so that a case can be created in the BCA case management system. Data about employees in the case management system are private data on individuals according to Minnesota Statutes, section 13.43, subd. 4.

The Executive Director will refer the individual to the agency at which the inappropriate use is alleged and will notify the Superintendent as needed.

If the data that were produced for the individual show a pattern of inappropriate use, the Executive Director will also consult with the CJIS Systems Officer (CSO) and the Director of the Training and Auditing Unit. Access by the user, the agency or both to a particular system or tool may be suspended during the investigation. Prior to any such suspension, the agency head will be notified of the action.

Recognizing that Minnesota Statutes, section 13.43 classifies data about alleged misconduct by an employee as private data, the Executive Director will request that the agency head consult with the Director of the Training and Auditing Unit prior to finalizing any disciplinary decisions so that the consequences related to data or system access can be coordinated. The CSO will have an opportunity to evaluate the general circumstances and determine if additional sanctions will be imposed by the BCA. Any data shared by the agency will be documented in the BCA case management system. The imposition of sanctions by the CSO may be appealed to the Superintendent of the BCA.

Allegations of inappropriate use from the head of an agency where the inappropriate use is alleged to have occurred

The head of an agency authorized to access data via the BCA systems and tools may contact either DPS Internal Affairs or the Director of the Training and Auditing Unit with a report of suspected inappropriate use. Internal Affairs will refer the agency to the Director of the Training and Auditing Unit.

After consulting with the agency about the basis for the allegations and obtaining initial facts, the Director of the Training and Auditing Unit will request that the agency send a written request for assistance with their investigation.

On receipt of the written request, appropriate queries in Archive Service are run and the data are reviewed. In addition, the request is recorded in the BCA case management system and the Training and Auditing Unit Director will inform the MNJIS Executive Director of the request. The Executive Director will notify the Superintendent, as needed, of these requests.

The Director of the Training and Auditing Unit will provide the agency with the data and will ask the agency to notify BCA of the findings of its investigation, to the extent possible given section 13.43, and to consult with BCA prior to taking any particular disciplinary action in response to what is found so that any consequences related to data or system access can be coordinated. The Director of the Training and Auditing Unit will provide assistance to the agency regarding access requirements for FBI and MNJIS systems.

When the report of the agency's findings from their investigation is received, the Director reviews its content. The findings are recorded in the BCA case management system along with any decision made by the CSO concerning sanctions. When the Director identifies a repeat offender, or the conduct is part of a pattern of possible criminal activity, or the offense appears to be egregious, the Director will meet with the CSO to discuss possible sanctions as provided in this policy. The CSO may concur with the findings and steps taken by the agency or may choose to impose additional sanctions. The imposition of sanctions by the CSO may be appealed to the Superintendent of the BCA.

Utilization of a methodology that identifies patterns of use for investigation and evaluation

The BCA has computer software that can analyze usage of queries involving data accessed over the BCA's secure network. The software can identify patterns of use that may be inappropriate according to this policy.

F. Process to Investigate and Evaluate Possible Inappropriate Use

General Process

- ✓ When data are received in Training and Auditing that indicate there may be inappropriate use, the BCA auditor will contact the agency head by telephone, explain what the data are and ask that an informal review be conducted to determine if the use is appropriate or not. If the agency head indicates to the BCA auditor that the use is appropriate, the matter ends. If

the agency head indicates that there may be or is inappropriate use, then the BCA auditor will open an audit.

- ✓ The agency will review a list of targeted transactions provided by their BCA auditor on a transaction worksheet. Within two weeks, the agency will provide a descriptive literal reason for each transaction, the user who ran each transaction, along with all public data that supports each of the transactions. The agency will be told that if it cannot respond within the two week period, an extension needs to be requested from the BCA auditor.
- ✓ The BCA auditor will send a reminder email to the agency on the 10th day, if the agency has not been in contact with the auditor.
- ✓ The agency will return the transaction worksheet with responses to the BCA auditor. The BCA auditor will review the responses supplied on the transaction worksheet.
- ✓ The failure of an agency to request an extension or reply within the two week time period will result in the determination that the access was inappropriate and immediately start the audit in the designated phase.
- ✓ The BCA auditor will issue audit findings using the audit application tool.
- ✓ The agency does have the right to provide a response to the audit findings as well as appeal any audit findings to the Director of the Training and Auditing Unit.

First inappropriate use

The Training and Auditing Unit will add a case into the BCA's case management system.

Once inappropriate use has been identified, the BCA auditor will retrieve the user's transactions for the 30 days prior to the inappropriate use. The transactions will be forwarded to the agency for immediate review and response – any inappropriate transactions will be included in the audit report.

The agency/user may be sanctioned as described later in this Policy.

An email will be sent to the agency head notifying them of BCA actions and to the DVS Data Practices Coordinator if DVS data are at issue.

If the user loses access, a follow-up audit will be conducted within 30 days of the user regaining access.

The audit is saved as noncompliant.

Second inappropriate use

The Training and Auditing Unit will add a case to the BCA's case management system.

A review of the user's transactions for the 30 days prior to the inappropriate use will occur. The transactions will be forwarded to the agency head for immediate review and response – any inappropriate transactions will be included in the audit report. The Director of the Training and Auditing Unit will request that the agency head consult prior to finalizing any discipline so that consequences can be coordinated.

The agency/user may be sanctioned as described later in this Policy.

An email will be sent to the agency head notifying them of BCA actions and to the DVS Data Practices Coordinator if DVS data are at issue.

A follow-up audit will be conducted within 30 days of the user regaining access.

The audit is saved as noncompliant.

Third inappropriate use

The Training and Auditing Unit will add a case to the BCA's case management system.

A review of other users' transactions or transactions in other repositories will be forwarded to the agency head for immediate review and response – any inappropriate transactions will be included in the audit report.

The Director of the Training and Auditing Unit will contact the agency to discuss an appropriate plan of action and will request that the agency head consult prior to finalizing any discipline so that consequences can be coordinated.

The agency/user may be sanctioned as provided later in this Policy.

An email will be sent to the agency head notifying them of BCA actions and to the DVS Data Practices Coordinator if DVS data are at issue.

The audit is saved as noncompliant.

G. Sanctions

Sanctions will be administered after a review and evaluation of the totality of the circumstances including the severity of the inappropriate use. Sanctions are cumulative over the career of the user or the life of the agency unless the user or agency demonstrates compliance through appropriate use for a six (6) year period. If six years of compliance is achieved, any future inappropriate use by the user or agency will be sanctioned as if there was no history of noncompliance. A user's history of inappropriate use follows the user to a new agency. Access by the user at a new agency will not be possible until the sanctioned user completes all elements of the sanction.

If one or more individual users at an agency are found to have inappropriate access to or use of one or more repositories or the secure network, the BCA will take the following steps, including the following sanctions.

1. Unauthorized access to the secure network by a user or agency will be terminated when possible.
2. Inappropriate access to a repository will place the agency in non-compliant status and the staff of the Training and Auditing Unit will work with the agency to achieve compliance. Tools used include follow-up audits, tutoring, coaching, mentoring and training.
3. The first violation by an individual user will result in training or the user's access will be suspended for a period not to exceed 5 working days or both.
4. A second violation by an individual user will result in suspension of access for a period not to exceed 30 calendar days and any other sanctions appropriate for the circumstances including, but not limited to, additional training or supervised system access.
5. A third violation by an individual user may result in one or more of the following: suspension of access for longer than 30 days, loss of access to other systems or tools that the individual uses, termination of access, or referral for criminal prosecution.
6. Notwithstanding items 3 through 5 above, the totality of the circumstances may be so egregious that stronger sanctions are warranted and will be imposed on a case-by-case basis.

If an agency has multiple users who are found to have inappropriate or unauthorized access to one or more repositories or the secure network, the following additional sanctions may be assessed against the agency.

A. Removal of access to one or more queries used to access information or functionalities such as Integrated Search Service or MNJIS Reports on Demand.
B. Restrict the number of users with access to one or more systems or tools for a period to time.
C. Disable system access for all users at the agency.
D. Notwithstanding items A through C above, the totality of the circumstances may be so egregious that stronger sanctions are warranted and will be imposed on a case-by-case basis.

The user or agency may appeal the imposition of sanctions to the Superintendent of the BCA.